UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, as described in Attachment A

Case No. 3:25-mc-00476

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C 841and 846	Possession and Conspiracy to Possess with Intent to Distribute
21 U.S.C. § 843(b)	Use of a Communication Facility to Commit or Facilitate Distribution of and Possession with Intent to Distribute a Controlled Substance

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Gillian Polinko, DEA Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 10:30 a.m / p.m *(specify reliable electronic means).*

Date: 04/28/2025

Judge's signature

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

The property to be searched is Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304, identified as the "**Subject Premises**." The **Subject Premises** is further described as a 10 foot by 20 foot storage unit labeled J21 within the secured area of the business named Highway 22 Storage. (See below photo of the Highway 22 Storage facility).

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises located at Storage unit No. J21, Highway 22 Storage, 130 50th Ave. NW, Salem, OR 97304 ("**Subject Premises**"), referenced in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of Title 21 U.S.C. §§ 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance, make it illegal to possess with intent to distribute a Controlled Substance, or to conspire to do so. Title 21, United States Code, Section 843(b) makes it unlawful to use a communication facility, such as a cellular telephone, to distribute controlled substances. The items to be seized cover the period of January 1, 2024, through the date of the execution of the warrant.

1. The items referenced above to be searched for, seized, and examined are:

a. Controlled substances, including but not limited to methamphetamine, fentanyl or cocaine, held in violation of 18 U.S.C 1956 and 21 U.S.C. Sections 841(a)(1) and 846;

b. Firearms, firearm accessories, and other dangerous weapons and ammunition;

c. Financial profits, proceeds and instrumentalities of trafficking in narcotics and money laundering, including U.S. Currency and other items of value.

d. Paraphernalia for packaging, smuggling, processing, diluting, manufacturing, weighing, and distributing controlled substances, for example: hidden compartments, scales, blenders, funnels, sifters, grinders, glass panes, mirrors, razor blades, plastic bags, heat sealing devices, and dilutants such as inositol, vitamin B12, etc.;

e. Books, records, receipts, notes, ledgers, and other documents relating to the manufacture and distribution of controlled substances; money laundering, communications between members of the conspiracy, and evidence of the use of apparently legitimate businesses to disguise profits.

f. Personal books and papers reflecting names, addresses, telephone numbers, and other contact or identification data relating to the manufacture, importation and distribution of controlled substances, and money laundering.

g. Financial records relating to controlled substances income and expenditures of money and wealth, to wit: money orders, wire transfer records, cashier's checks and receipts, account records, passbooks, tax records, safe deposit box keys and records, checkbooks, and check registers, as well as precious metals and gems such as gold, silver, diamonds, etc. purchased/acquired between January 1, 2024, and the present;

h. Items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the premises, including but not limited to canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys;

j. Other cellular telephones, computers and other electronic devices capable of storing data that constitutes evidence or the instrumentality of drug dealing and conspiracy to do the same may be seized so the government may apply for search warrants for any other devices located at the **Subject Premises**;

k. Latent prints and identifying material from items at the premises, including the fingerprints of the unidentified individuals located at the **Subject Premises**.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF GILLIAN POLINKO

Affidavit in Support of an Application Under Rule 41 for a Search Warrant

I, Gillian Polinko, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7). I am currently employed as a Special Agent ("SA") with the United States Drug Enforcement Administration ("DEA"), and assigned to the District Office in Albuquerque, New Mexico. I have been a SA since April of 2019. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am empowered by law to conduct investigations and to make arrests for criminal offenses, to include those enumerated in 18 U.S.C. § 2516. I graduated from the DEA Training Academy in Quantico, Virginia, after receiving approximately sixteen weeks of specialized narcotics related training. While at the DEA Training Academy I became familiar with how controlled substances are consumed, manufactured, packaged, marketed, and distributed. I received training on surveillance and counter-surveillance operations, undercover operations, confidential source operations, criminal law, and investigations involving federal electronic surveillance statutes, to include Title III wiretaps, drug identification, search warrant executions, and vehicle stops.

2. My experience as a SA includes, but is not limited to, conducting surveillance, interviewing witnesses, writing affidavits for and executing search and seizure warrants, conducting extensive toll analysis, debriefing defendants and confidential sources and working with undercover agents and informants. I have received training and have experience in the

investigation of violations of the federal drug and money laundering laws, including the offenses listed below. As a result, I am familiar with matters including, but not limited to, the means and methods used by drug traffickers and drug trafficking organizations to purchase, transport, store, and distribute illegal drugs and to hide profits generated from those transactions. I also have experience in analyzing and interpreting drug codes and cryptic dialogues used by drug traffickers. I have spoken to other law enforcement officers with similar experience.

3. This case is being investigated by the DEA. I have personally participated in the investigation. I make this affidavit based on my participation in the investigation, and based on reports and information made available to me by other agents and Task Force Officers ("TFOs"), as well as other law enforcement authorities. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge or surrounding facts pertaining to this matter.

4. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises described as the following:

a. **Subject Premises**: Storage unit No. J21, located at Highway 22 Storage, 130 50th Ave. NW Salem, OR 97304, being used by an individual, referred to as Heriberto SALAZAR AMAYA ("HSA"). **Subject Premises** is described in Attachment A and incorporated herein,

for evidence, contraband, fruits, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1), 846, and 843(b), to-wit: the distribution and possession with intent to distribute a controlled substance, conspiracy to distribute and possess with intent to distribute a controlled substance, and the use of a communication facility in furtherance of the distribution of a

controlled substance (hereinafter the "Target Offenses"). As set forth below, I have probable cause to believe that such property and items, as described in Attachment B hereto, including any digital devices or electronic storage media, are currently located at the **Subject Premises**, which is located within the District of Oregon.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offenses

6. I have probable cause to believe that evidence of the below listed violations will be found within the premises to be searched as they are described in Attachment A:

a. Title 21, United States Code, Section 841(a)(1), Distribution and Possession with Intent to Distribute a Controlled Substance;

b. Title 21, United States Code, Section 846, Conspiracy to Distribute and Possess with Intent to Distribute a Controlled Substance; and,

c. Title 21, United States Code, Section 843, Use of a Communication Facility in Furtherance of a Drug Crime (Distribution of a Controlled Substance).

Statement of Probable Cause - Background

7. DEA is conducting a criminal investigation of HSA, and his drug trafficking organization ("DTO"), who have conspired to distribute, and are distributing, controlled substances in New Mexico, Nevada, and Colorado, in violation of 21 U.S.C. §§ 841(a)(1) and 846. This investigation has included wiretaps on a series of phones used by HSA. Agents began intercepting wire and electronic communications over several phones used by HSA beginning in August 2024. On April 19, 2025, the wiretaps ended on three phones being used by HSA. Throughout the course of this investigation, agents have identified numerous phone numbers, vehicles, and residences that HSA and members of his DTO use to facilitate their drug trafficking activities. Agents have learned that HSA often rents Airbnb and VRBO properties, both for himself and his couriers, and has been observed staying in Phoenix, Arizona, Lakewood, Colorado, Las Vegas, Nevada, Ogden, Utah, and now Salem, Oregon since the investigation commenced in August 2024. Given this posture, Agents believe that HSA's transiency is designed to evade law enforcement detection. Furthermore, since the investigation commenced in August 2024, agents have identified a total of fifteen (15) phone devices associated with HSA, each with a different phone number, which HSA has used to facilitate his drug trafficking activities.

8. As part of this investigation, agents identified HSA as the user of cellphone with number (505) 906-0877 ("HSA PHONE 1"). Agents confirmed HSA as the user of HSA PHONE 1 on September 11, 2024, in Las Vegas, Nevada. There, Agents observed HSA at a restaurant that corresponded to an active ping on HSA Phone 1. Agents then conducted a ruse call and observed HSA answer HSA PHONE 1. Agents then used common call analysis to

identify subsequent HSA phones as he progressed through new devices. Agents also were able to confirm HSA used the subsequent devices through his voice, common code words, identical customers, pings in relation to HSA's known vehicles and travel, as well as pings associated with HSA's residences.

9. Based on my training and experience, I know that drug traffickers often cycle through devices and/or phone numbers to evade law enforcement detection. Additionally, based on training and experience, including familiarity with the HSA DTO, drug traffickers also compartmentalize the organization by using specific phones for different levels of operators with the DTO, allowing HSA to drop a phone if and when a customer is interdicted by law enforcement.

Arrest of Bruce SEDILLO – Drug Customer of HSA

10. In November 2024, agents intercepted communications over (505) 321-8920 ("SEDILLO PHONE 1")[1] between SEDILLO and HSA, who was using (505) 288-0537 ("HSA PHONE 8") at this time. During these calls, HSA and SEDILLO arranged a drug transaction at SEDILLO's residence in Albuquerque, NM. The transaction was expected to occur between SEDILLO and a courier for the HSA DTO. These communications led agents to believe SEDILLO was expected to receive over 100,000 fentanyl pills from HSA through his courier. Agents established surveillance at SEDILLO's residence in conjunction with the communications between SEDILLO and HSA, where they observed an HSA DTO courier

[1] Interceptions took place pursuant to a lawful search warrant authorizing the interception of wire and electronic communications over SEDILLO PHONE 1. On October 31, 2024, United States District Judge James O. Browning authorized the interception of wire and electronic communications over SEDILLO PHONE 1. *See* MR-24-2014.

deliver the suspected narcotics to SEDILLO's residence. Two days later, agents executed a search warrant at SEDILLO's residence and seized approximately 150,000 suspected fentanyl pills with labels that included "Leon" and "GSV," approximately $71,950.00 U.S.C., and multiple firearms and silencers:

11. Agents conducted a post-arrest interview with SEDILLO. During the interview, SEDILLO identified HSA as a primary operator for the Sinaloa Cartel. SEDILLO also identified one of HSA's known couriers, Cesar ACUNA-MORENO ("ACUNA"), as the individual who provided the "Leon" and "GSV" fentanyl pills located by law enforcement in his residence. SEDILLO further explained that the fentanyl pills, which again were marked with "Leon" and "GSV" labels, were supplied by HSA, whom he only knew as "Juan." Based on the investigation into the HSA DTO, law enforcement confirmed that "Juan" is a known alias that HSA uses for his drug customers. During the post-arrest interview, SEDILLO was able to recognize an individual that was HSA after viewing a 6-pack photo array. However, SEDILLO stated that he only knew him as a member of the DTO. SEDILLO continued that he had seen HSA only once

before and that encounter occurred years prior. Law enforcement did not notify SEDILLO that he was viewing a picture of HSA.

12. As stated above, throughout the course of this investigation, HSA has repeatedly changed phone numbers and repeatedly changed locations in response to police pressure and other factors, which is consistent with the common practice of drug traffickers. Drug traffickers often change phone numbers and physical devices in an attempt to thwart law enforcement. However, in doing so, drug traffickers are constrained by the necessity to alert their various customers and suppliers as to the new phone number. Based on training and experience, agents are aware that a drug trafficker will often change phone numbers and then utilize the "new" phone number to contact the customer and/or source of supply to inform the customer and/or source of supply of the change. In this case, HSA behaved in this exact manner following the apprehension of SEDILLO and the seizure of approximately 150,000 fentanyl pills. HSA immediately dropped (505) 288-0537 (HSA PHONE 8) and later contacted his other customers by phone, which law enforcement identified through common call analysis as well as through other intercepted communication.

13. For example, right before HSA dropped HSA PHONE 8, law enforcement intercepted a call between HSA and a customer, where HSA notified the customer that he would be providing a new line shortly. Then, on November 16, 2024, agents intercepted an SMS text message to Vincent MONTOYA ("MONTOYA"), a known customer of the HSA DTO (discussed more below). That message was sent from "Juan," and stated that the sending number was Juan's new line. Based on the investigation, and confirmed by SEDILLO, agents know Juan to be HSA.

HSA Travels to Salem, Oregon in January 2025

14. On January 5, 2025, agents observed the geolocation data for (505) 524-4990 ("HSA PHONE 11"), (720) 415-7496 ("HSA PHONE 12"), and (720) 289-0736 ("HSA PHONE 13"), all which were identified and connected to HSA through common call analysis, pings, and surveillance. The data indicated that these three phones appeared to be traveling towards the Oregon area from the Ogden, Utah area. Additionally, agents intercepted phone calls over HSA PHONE 13 with (928) 290-9528, a phone number believed to be used by George NAVARRETE ("NAVARRETE"), indicating that he was traveling in tandem with NAVARRETE, a known criminal associate and member of the HSA DTO.[2] Prior to January 5, 2025, agents had never observed HSA travel to Oregon.

15. On January 11, 2025, agents observed the geolocation data for HSA PHONE 11, HSA PHONE 12, and HSA PHONE 13 traveling out of the Salem, OR area and ultimately arrive to Phoenix, AZ on January 12, 2025. Agents have identified Phoenix, AZ as HSA's source city for the narcotics he distributes throughout Albuquerque, NM, Denver, CO, and Las Vegas, NV. For example, during the investigation, agents have intercepted calls where HSA informs customers that he operates in multiple cities such as Denver and Colorado Springs. Agents have worked in conjunction with Denver DEA agents and have corroborated HSA dispatching couriers to customers in Denver, consistent with HSA's drug trafficking in Albuquerque. Agents have observed HSA travel in tandem from Phoenix to the New Mexico border with a suspected load vehicle, and then passed the load vehicle off to his couriers, further indicating his drug

[2] Agents have reviewed several bank statements that show cash transfers between HSA and NAVARRETE. Agents also have conducted surveillance on NAVARRETE during drugs transactions conducted between members of the HSA DTO.

trafficking in multiple states and jurisdictions. Additional examples of HSA drug trafficking follow.

Oregon Traffic Stop of HSA on February 7, 2025

16. On February 7, 2025, agents received a call from an Oregon state police officer who observed a silver Ford truck bearing NM temporary tag 25T-039432 and a gray GMC Yukon bearing NM license plate BYPG07 traveling in tandem in La Grande, Oregon. According to New Mexico MVD, plate 25T-039432 is registered to "RAMIREZ NAVARRETE on a silver 2021 Ford F-150," and plate BYPG07 is registered to "Danny CALLEJA at 7 Venado Ct. Los Lunas, NM," on a 2023 gray GMC Yukon SUV. Additionally, during this time, agents were receiving GPS ping location data for HSA PHONE 11, HSA PHONE 12, and HSA PHONE 13, and (928) 290-9528, which placed all the devices traveling in the area of La Grande, Oregon.

17. The officer informed agents that he conducted a traffic stop of the silver F-150 due to the temporary tag on the vehicle. The officer identified the driver as HSA, who provided his NM driver's license and the registration of the vehicle. HSA also provided his phone number as (720) 289-0736 ("HSA PHONE 13") to the officer and stated that he would be staying with his family at 855 Rumsey NW, Salem, Oregon, for approximately two months. Additionally, HSA provided the registration for the silver F-150, which is in NAVARRETE's name, and provided NAVARRETE's phone number as (928) 290-9528, thereby confirmed the active ping on NAVARRETE's phone. The officer further stated that he observed a large amount of currency in plain view, to which HSA stated that it was approximately $15,000 U.S.C.

/ / / /

/ / / /

Agents Identify the HSA Residence

18. On March 11, 2025, the Honorable David Herrera Urias, District Judge for the District of New Mexico, approved an order authorizing the renewed interception of wire and electronic communications occurring to and from HSA PHONE 11 and HSA PHONE 12. Agents have identified HSA PHONE 11 as a phone HSA uses to communicate with his drug customers residing in Albuquerque, NM. Agents have identified HSA PHONE 12 as a phone HSA uses to communicate with his drug customers residing in the Denver, CO area. Additionally, the Court authorized the seizure of location data related to HSA PHONE 11 and HSA PHONE 12 for the period of interception. Interceptions concluded on HSA PHONE 11 and HSA PHONE 12 on April 10, 2025.

19. On March 20, 2025, the Honorable David Herrera Urias, District Judge for the District of New Mexico, approved an order authorizing the initial interception of wire and electronic communications occurring to and from (360) 601-9164 ("HSA PHONE 15"). Agents have identified HSA PHONE 15 as a phone HSA uses to communicate with his drug couriers, Mexican sources of supply, and family. Additionally, the Court authorized the seizure of location data related to HSA PHONE 15 for the period of interception. Interceptions concluded on HSA PHONE 15 on April 19, 2025.

20. On April 1, 2025, at approximately 1:13 p.m., agents received a phone call between (503) 362-3601, a phone number used by VELAZCO, and HSA PHONE 15, used by HSA. Agents believe VELAZCO is the significant other of HSA. During this phone call, VELAZCO informed HSA that the electricity went out at their house and HSA states that he will check to see if they can re-connect the services.

21. On this same day, at approximately 1:15 p.m., agents received an outgoing phone call (session 290) over HSA PHONE 15, used by HSA, and (503) 362-3601, the phone number belonging to Salem Electric. During this phone call, HSA provided his residential address as "137 Greencrest Street northeast," (the "HSA Residence") and stated that he was inquiring about getting new services for this address. The phone call continued and HSA was advised that the electric services would be through "PGE." The phone call ended shortly thereafter.

22. At approximately 1:18 p.m., agents intercepted a phone call over HSA PHONE 15, used by HSA, and (800) 743-5000, the phone number belonging to Pacific Gas & Electric Company ("PGE"). During this phone call, HSA advised that he is inquiring about a new service at "137 Greencrest Street northeast, Salem Oregon 97301" (HSA Residence). HSA also advised that his name is "Heriberto Salazar" and that it is his first time having services with PGE. HSA further stated that he had been living at the residence for the past week but he received the keys on the 1st day of March. The conversation continued and HSA provided more personal information, including his full name, "Heriberto Salazar Amaya," and stated that he has an ITIN number. Additionally, HSA provided his New Mexico driver's license number as "519447461." The call continued and HSA provided a cell phone number, which is consistent with HSA PHONE 15, and an email address of Heribertosalazar0707@gmail.com. HSA also provides his date of birth as "August 15, 1988." This is the actual birthday of HSA. HSA further explained that he is currently renting the residence (HSA Residence) and the phone call ends shortly after.

23. Based on the above-mentioned phone calls, Albuquerque DEA agents requested assistance from the DEA Salem Resident Office to locate the HSA Residence and observe what vehicles were present. On April 2, 2025, DEA Salem officers conducted a spot check

surveillance at the HSA Residence, and observed an orange Ford Raptor truck bearing Colorado license plate DYX-O84 parked in the driveway. According to Colorado Motor Vehicle Department, license plate DYX-O84 is registered to Hortencia TIZCARENO ("TIZCARENO") at 4115 Dunkirk Ct, Denver, CO 80249 on a 2023 Orange Ford F-150 Raptor pickup truck. Furthermore, agents had previously identified and observed HSA operating this vehicle in Las Vegas, NV in September 2024. Agents are also aware that HSA operates several vehicles registered under TIZCARENO's name and have identified numerous vehicles utilized by the HSA DTO that are registered to TIZCARENO. Based on these observations, DEA Salem installed a covert camera facing the HSA Residence in an effort to monitor the residence.

Wiretap Intercepts Show HSA's Drug Trafficking Activities are Ongoing

24. On March 25, 2025, at approximately 4:50 p.m., agents intercepted a phone call between HSA PHONE 11, confirmed to be used by HSA as mentioned above, and (505) 420-8816 ("MONTOYA PHONE"), used by Vincent MONTOYA ("MONTOYA"), a drug customer of HSA's in Albuquerque, NM. During this call, HSA and MONTOYA discussed an unknown quantity of narcotics, specifically "Leons" and the "GSVs", that MONTOYA needed to purchase from HSA. It should be noted here, as mentioned above, that law enforcement seized approximately 150,000 fentanyl pills from SEDILLO's house with labels that included "Leon" and "GSV," therefore agents believe MONTOYA was referring to fentanyl pills unique to the HSA DTO in this call. Additionally, during this call, HSA also informed MONTOYA that the "GSV" and the "Leons" are the "best ones" he has, which agents believe HSA is referring to the quality of the fentanyl pills. MONTOYA indicated that he wanted to purchase narcotics from HSA and would call him later that same day.

25. Later that night, at approximately 9:36 p.m., agents intercepted a phone call between HSA and MONTOYA over HSA PHONE 11, where both parties agreed to meet the following day for the purpose of conducting a drug transaction.

26. On March 26, 2025, at approximately 6:26 p.m., agents intercepted a phone call between HSA and MONTOYA, over HSA PHONE 11. During this call, MONTOYA informed HSA that he would be ready to conduct the drug transaction in thirty minutes. Immediately following this call, agents intercepted a phone call between HSA and ACUNA, over HSA PHONE 14. During this call, HSA instructed ACUNA, the very same courier who delivered to SEDILLO above, to meet with "la gringa" at 7:15 p.m., to which ACUNA acknowledged HSA and the phone call ended shortly thereafter. Agents believe HSA was referring to MONTOYA as "la gringa" in this call based on the prior call HSA had with MONTOYA regarding a drug transaction set to occur in thirty minutes. At this time, agents established surveillance in the vicinity of MONTOYA's residence located in northwest Albuquerque, NM. Agents also established surveillance in a residential area located at La Cienega St NW and Palo Duro Ave NW, where agents had previously observed a drug transaction occur between MONTOYA and ACUNA.

27. At approximately 7:14 p.m., agents observed ACUNA, driving a gray Honda CR-V, arrive to a residential area located at La Cienega St NW and Palo Duro Ave NW and park curbside. At approximately 7:16 p.m., agents observed MONTOYA exit from his residence and load a suitcase into a white Dodge Ram, which is a vehicle MONTOYA is known to use. Moments later, agents observed MONTOYA depart from his residence.

28. At approximately 7:20 p.m., agents observed MONTOYA arrive to the residential area where ACUNA remained waiting. At this time, agents observed MONTOYA exit from his vehicle and retrieve the suitcase out of the rear driver's seat. Simultaneously, agents observed ACUNA exit from the Honda CR-V and retrieve a black tub with a yellow lid from the rear driver's seat. Agents then observed both parties make the exchange of the suitcase and the black tub with yellow lid in the middle of the residential street and walk back to their respective vehicles. Moments later, both parties departed from the area. Based on these observations in conjunction with the intercepts over HSA PHONE 11 and HSA PHONE 15, agents believe MONTOYA ordered a quantity of narcotics from HSA and ACUNA facilitated the drug transaction on HSA's behalf.

29. On April 3, 2025, at approximately 12:36 p.m., agents intercepted a phone call between HSA PHONE 11, used by HSA, and (505) 948-0721 ("ANESI PHONE"), used by David ANESI ("ANESI"), a drug customer of HSA's in Albuquerque, NM. During this call, ANESI informs HSA that he has money for the narcotics he received from HSA on a previous drug transaction. In this call, ANESI further states, "I'm gonna need… uh, the same thing," to which HSA affirms. ANESI then clarifies, "not the t-shirt though," which agents believe to be a common drug code for a kilogram of cocaine. ANESI then asks HSA if he has the "waters" and that he will need one of those too. Based on my training and experience from prior investigations, agents believe the term "water" is a common drug code for methamphetamine. HSA then informs ANESI that his guy is out of town and that he will arrive in Albuquerque around seven (7) or eight (8) p.m. At this time, agents observed the tracker location data for the

grey Honda CR-V[3] was placing the vehicle in the Denver, CO area. Additionally, agents believe that ACUNA typically utilizes the Honda CR-V as his primary vehicle.

30. Later this same day, agents intercepted a phone call between HSA and ANESI over HSA PHONE 11. In this call, HSA advises ANESI that he will check with his courier (ACUNA) to see how far from Albuquerque he is. Immediately following the call with ANESI, agents intercepted a phone call between HSA and ACUNA over HSA PHONE 15, where HSA states, "I can tell David if he wants to meet up late, if not, until tomorrow then. Right?" Agents believe HSA is referring to David ANESI and that ACUNA, the very same courier who delivered to SEDILLO and MONTOYA above, will be the one to deliver the narcotics on HSA's behalf.

31. Throughout the evening hours, agents were monitoring the tracking device located on the Honda CR-V and observed the Honda CR-V traveling eastbound on Paseo Del Norte NE towards ANESI's residence located in northeast Albuquerque, NM. At this time, agents established surveillance at ANESI's residence. At approximately 10:53 p.m., agents observed the Honda CR-V arrive to ANESI's residence and park in the driveway. At approximately 10:57 p.m., agents observed the garage of ANESI's residence open and ANESI standing in the garage. Agents then observed ACUNA exit from the driver's seat of the Honda CR-V, carrying a dark-colored backpack, and enter the residence through the garage, the garage closing shortly after. At approximately 11:13 p.m., agents observed the garage open and ACUNA exit, carrying the same dark-colored backpack, and enter the driver's seat of the Honda CR-V. Surveillance was subsequently terminated once the Honda CR-V departed from ANESI's

[3] Refer to MR-25-484.

residence. Based on the intercepted communications, in conjunction with surveillance, agents believe HSA instructed ACUNA to deliver the narcotics ANESI ordered to ANESI's residence. Agents believe ACUNA complied. Accordingly, HSA is continuing to facilitate drug transactions and send couriers on his behalf to deliver the narcotics.

32. On April 16, 2025, at approximately 6:26 p.m., agents intercepted a phone call between HSA and ACUNA, over HSA PHONE 15. During this phone call, HSA instructs ACUNA, the very same courier who delivered to SEDILLO, ANESI, and MONTOYA above, to get "la gringa's" order ready, to which ACUNA asks HSA if he can tell him what the order is going to be. HSA further explains that it will be "diez papas" (10 potatoes), "treinta tres cajas" (33 boxes), and to put in "diez Leones" (10 Leones). It should be again noted here, as mentioned above, that law enforcement seized approximately 150,000 fentanyl pills from SEDILLO's house with labels that included "Leon." Furthermore, throughout the course of this investigation, agents have learned that HSA communicates with his couriers using coded language when referring to narcotics. Agents believe this is in an effort to thwart law enforcement detection. However, agents have been able to identify various code words relating to certain narcotics. Agents believe "potatoes" is in reference to pound-quantities of methamphetamine and "boxes" is in reference to a bundle of 10,000 suspected fentanyl pills. As just stated, agents also believe "Leones" is in reference to the quality or potency of specific fentanyl pills as brand unique to HSA, that HSA is providing to his customer (la gringa). ACUNA acknowledges HSA and asks what time, to which HSA states, "7:30." HSA further states that "Bacardi" is going to "give you half and owe half," which agents believe HSA is referring to money owed for the narcotics. Based on the forgoing, agents believe HSA continues to facilitate drug transactions.

Agents Further Link HSA to HSA Residence

33. On April 23, 2025, at approximately 10:32 a.m., agents began receiving geolocation data for HSA PHONE 15, which placed the device in close proximity of the HSA Residence.[4] At this time, agents reviewed electronic surveillance at the HSA Residence from the night of April 22, 2025. At approximately 9:20 p.m., agents observed a male, wearing a black t-shirt and black shorts, and a female, wearing a dark-colored t-shirt and black pants, exit from the vicinity of the front entrance of the HSA Residence and walk towards the orange F-150 parked in the driveway. Agents observed that the male and female matched the description of HSA and VELAZCO, however, due to the lack of daylight at this time, agents were unable to confirm. Agents observed the female return back to the HSA Residence and the male enter the driver's seat of the orange F-150 and re-position the vehicle in the driveway. Agents then observed the male exit from the driver's seat and walk out of view, towards the street. Moments later, agents observed a gray Ford Bronco Raptor reverse onto the driveway of the HSA Residence and park. Agents observed that this vehicle matched the description of a gray Ford Bronco Raptor bearing CO license plate EQAS01, that HSA has been observed driving on prior surveillances. Agents observed the male open the trunk of the gray Bronco, appearing to unload items, and take them inside the HSA Residence.

34. On April 23, 2025, during the late-morning hours, agents observed, via electronic surveillance, a female and male exit from the vicinity of the front entrance of the HSA Residence. At this time, agents were able to positively identify and confirm that HSA and

[4] Prior to receiving geolocation data for HSA PHONE 15, agents last knew of HSA's location being in the Las Vegas, NV area as of April 19, 2025.

VELAZCO are indeed the male and female that are present at the HSA Residence. Furthermore, agents with DEA Salem conducted a spot-check surveillance of the HSA Residence later this same day and observed that the gray Bronco was parked in the driveway and was bearing CO license plate EQAS01. According to Colorado MVD, license plate EQAS01 is registered to Jose Luis TIZCARENO at 4115 N Dunkirk Ct, Denver, CO 80249, on a 2024 gray Ford Bronco, which is the same vehicle HSA has been observed operating in the past. Based on the foregoing, I believe HSA is currently residing at the HSA Residence. As stated above, law enforcement began receiving geolocation data for HSA PHONE 15 on April 23, 2025, which placed HSA at the HSA Residence on the night of April 23, 2025, the morning and night of April 24, 2025, and the morning of April 25, 2025. This location data was also confirmed by a pole camera located at the HSA Residence, which places HSA's vehicle in the driveway.

35. On April 24, 2025, HSA was indicted in the District of New Mexico along with thirteen other individuals on a 12-count indictment. HSA was charged with the following: Count 1: 21 U.S.C. § 846: Conspiracy; Count 10: 8 U.S.C. §§ 1326(a) and (b): Reentry of a Removed Alien; Count 11: 8 U.S.C. § 1324a(a)(1)(A): Unlawful Employment of Illegal Alien; and Count 12: 8 U.S.C. § 1324(a)(1)(A)(v)(I): Conspiracy to Harbor Illegal Aliens.[5]

Agents Identify the Storage Unit J21

36. On April 28, 2025, agents executed a court-authorized search warrant on the HSA Residence. There, agents located HSA, three other adults (HSA's girlfriend, her mom, and the teenage daughter), HSA's infant daughter, large amounts of cash, seven (7) cellular devices, and

[5] SEDILLO, MONTOYA, ACUNA, ANESI, and NAVARRETE are co-defendants in the indictment, among others.

documents related to a storage facility at Highway 22 Storage (**Subject Premises**) leased by HSA in his name.

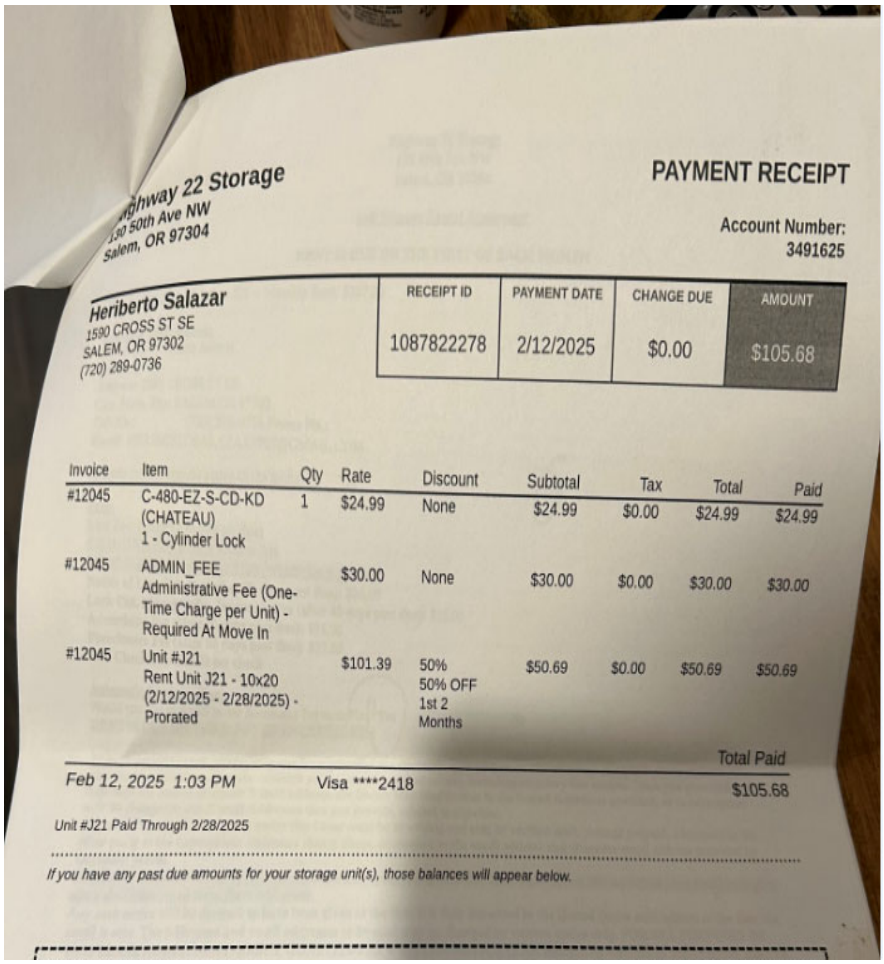
Bulk cash seized on April 28, 2025, from search of the HSA Residence in Salem, Oregon

/ / / /

/ / / /

/ / / /

/ / / /



...hway 22 Storage
...30 50th Ave NW
Salem, OR 97304

PAYMENT RECEIPT

Account Number:
3491625

Heriberto Salazar
1590 CROSS ST SE
SALEM, OR 97302
(720) 289-0736

RECEIPT ID	PAYMENT DATE	CHANGE DUE	AMOUNT
1087822278	2/12/2025	$0.00	$105.68

Invoice	Item	Qty	Rate	Discount	Subtotal	Tax	Total	Paid
#12045	C-480-EZ-S-CD-KD (CHATEAU) 1 - Cylinder Lock	1	$24.99	None	$24.99	$0.00	$24.99	$24.99
#12045	ADMIN_FEE Administrative Fee (One-Time Charge per Unit) - Required At Move In		$30.00	None	$30.00	$0.00	$30.00	$30.00
#12045	Unit #J21 Rent Unit J21 - 10x20 (2/12/2025 - 2/28/2025) - Prorated		$101.39	50% 50% OFF 1st 2 Months	$50.69	$0.00	$50.69	$50.69

Total Paid
$105.68

Feb 12, 2025 1:03 PM Visa ****2418

Unit #J21 Paid Through 2/28/2025

If you have any past due amounts for your storage unit(s), those balances will appear below.

*Copy of receipt for rental of **Subject Premises** from search of the HSA Residence in Salem, Oregon*

/ / / /

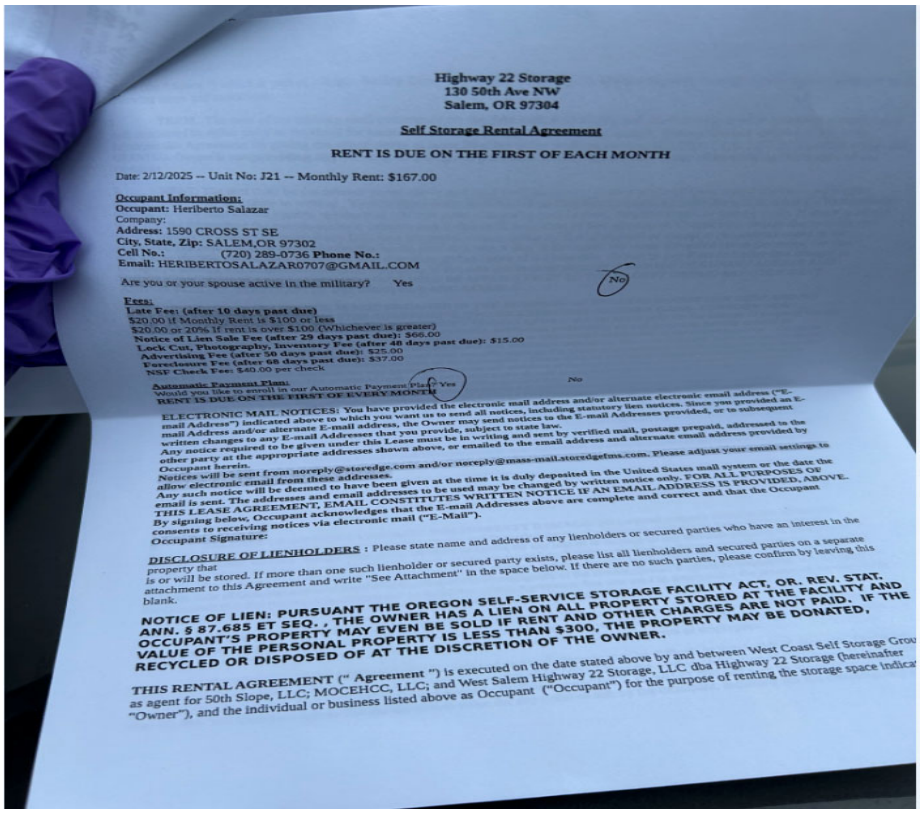
/ / / /

/ / / /

/ / / /

/ / / /

/ / / /



Highway 22 Storage
130 50th Ave NW
Salem, OR 97304

Self Storage Rental Agreement

RENT IS DUE ON THE FIRST OF EACH MONTH

Date: 2/12/2025 -- Unit No: J21 -- Monthly Rent: $167.00

Occupant Information:
Occupant: Heriberto Salazar
Company:
Address: 1590 CROSS ST SE
City, State, Zip: SALEM,OR 97302
Cell No.: (720) 289-0736 Phone No.:
Email: HERIBERTOSALAZAR0707@GMAIL.COM

Are you or your spouse active in the military? Yes No

Fees:
Late Fee: (after 10 days past due)
$20.00 if Monthly Rent is $100 or less
$20.00 or 20% if rent is over $100 (Whichever is greater)
Notice of Lien Sale Fee (after 29 days past due): $66.00
Lock Cut, Photography, Inventory Fee (after 48 days past due): $15.00
Advertising Fee (after 56 days past due): $25.00
Foreclosure Fee (after 68 days past due): $37.00
NSF Check Fee: $40.00 per check.

Automatic Payment Plan:
Would you like to enroll in our Automatic Payment Plan? Yes No
RENT IS DUE ON THE FIRST OF EVERY MONTH

ELECTRONIC MAIL NOTICES: You have provided the electronic mail address and/or alternate electronic email address ("E-mail Address") indicated above to which you want us to send all notices, including statutory lien notices. Since you provided an E-mail Address and/or alternate E-mail address, the Owner may send notices to the E-mail Addresses provided, or to subsequent written changes to any E-mail Addresses that you provide, subject to state law.
Any notice required to be given under this Lease must be in writing and sent by verified mail, postage prepaid, addressed to the other party at the appropriate addresses shown above, or emailed to the email address and alternate email address provided by Occupant herein.
Notices will be sent from noreply@storedge.com and/or noreply@mass-mail.storedgefms.com. Please adjust your email settings to allow electronic email from these addresses.
Any such notice will be deemed to have been given at the time it is duly deposited in the United States mail system or the date the email is sent. The addresses and email addresses to be used may be changed by written notice only. FOR ALL PURPOSES OF THIS LEASE AGREEMENT, EMAIL CONSTITUTES WRITTEN NOTICE IF AN EMAIL ADDRESS IS PROVIDED, ABOVE.
By signing below, Occupant acknowledges that the E-mail Addresses above are complete and correct and that the Occupant consents to receiving notices via electronic mail ("E-Mail").
Occupant Signature:

DISCLOSURE OF LIENHOLDERS : Please state name and address of any lienholders or secured parties who have an interest in the property that is or will be stored. If more than one such lienholder or secured party exists, please list all lienholders and secured parties on a separate attachment to this Agreement and write "See Attachment" in the space below. If there are no such parties, please confirm by leaving this blank.

NOTICE OF LIEN: PURSUANT THE OREGON SELF-SERVICE STORAGE FACILITY ACT, OR. REV. STAT. ANN. § 87.685 ET SEQ., THE OWNER HAS A LIEN ON ALL PROPERTY STORED AT THE FACILITY AND OCCUPANT'S PROPERTY MAY EVEN BE SOLD IF RENT AND OTHER CHARGES ARE NOT PAID. IF THE VALUE OF THE PERSONAL PROPERTY IS LESS THAN $300, THE PROPERTY MAY BE DONATED, RECYCLED OR DISPOSED OF AT THE DISCRETION OF THE OWNER.

THIS RENTAL AGREEMENT (" Agreement ") is executed on the date stated above by and between West Coast Self Storage Grou as agent for 50th Slope, LLC; MOCEHCC, LLC; and West Salem Highway 22 Storage, LLC dba Highway 22 Storage (hereinafter "Owner"), and the individual or business listed above as Occupant ("Occupant") for the purpose of renting the storage space indica

*Rental Agreement for **Subject Premises** recovered from search of the HSA Residence in Salem, Oregon*

37. Based upon my training, experience, and participation in this and other investigations involving drug trafficking, along with conversation with other experienced investigators and law enforcement agents with whom I work, and interviews of individuals who have been involved in the trafficking of drugs, I have learned and know the following:

a. Drug traffickers often utilize "stash houses" and other off-site facilities such as storage units to conceal their illegal activities and contraband and these "stash locations" may or may not be their actual residence, such was when a storage unit is used. Drug traffickers often utilize multiple "stash locations" to conceal large amounts of drugs, drug proceeds, or other contraband and to keep law enforcement and/or competitors from finding the same.

b. I know that drug dealing is a dangerous business and that drug traffickers regularly arm with firearms themselves to protect themselves, their drugs, and the cash they make from selling drugs from being robbed and stolen.

c. It is common to find papers, letters, billings, documents, and other writings, which show ownership, dominion, and control of businesses, residences, and/or vehicles in the residences and vehicles of drug traffickers. Items of personal property that tend to identify the person(s) in control or ownership of the **Subject Premises** also include canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, keys, financial papers, rental receipts and property ownership papers, personal and business telephone and address books and telephone toll records; and other personal papers or identification cards in the names of subjects involved in the criminal activity being investigated.

d. It is common for drug dealers to secrete proceeds of illegal drug sales and records of illegal drug transactions in secure locations within stash locations for their ready access and to conceal them from law enforcement authorities.

e. Drug traffickers amass large proceeds from the illegal sale of controlled substances that they attempt to legitimize. To accomplish these goals, drug traffickers utilize financial institutions and their attendant services, securities, cashier's checks, safe deposit boxes, money drafts, real estate, shell operations, and business fronts. Persons involved in drug trafficking and/or money laundering keep papers relating to these activities for future reference, including Federal and State tax records, loan records, mortgages, deeds, titles, certificates of ownership, records regarding investments and securities, safe deposit box rental records and

keys, and photographs. I know from my training and experience that often items of value are concealed by persons involved in large-scale drug trafficking inside of safes, lock boxes, and other secure areas within stash locations, including storage units.

f. Drug traffickers very often place assets in names other than their own to avoid detection of these assets by government agencies, and that even though these assets are in other individual or business names, the drug dealers actually own and continue to use these assets and exercise dominion and control over them.

g. Unexplained wealth is probative evidence of crimes motivated by greed, in particular, illegal trafficking in drugs.

h. Drug traffickers often document aspects of their criminal conduct through photographs or videos of themselves, their associates, their property, and their product. Drug traffickers usually maintain these photographs or videos in their possession.

i. Drug traffickers must maintain large amounts of United States currency in order to maintain and finance their on-going illegal drug trafficking business.

j. Drug traffickers utilize mobile electronic devices including cellular telephones and other wireless communication devices for the purpose of maintaining their illegal trafficking business. Such equipment often contains evidence of these illegal activities.

k. It is common for drug dealers to possess additional drugs for purposes of further distribution, as well as drug paraphernalia and other items which are associated with the distribution and possession with the intent to distribute controlled substances such as scales, hidden compartments, blenders, funnels, sifters, grinders, glass panes, mirrors, razor blades,

plastic bags, heat sealing devices, and dilutants such as inositol, vitamin B12, etc., within their residences, stash houses (storage locations), and vehicles.

l. Distributors of drugs frequently try to conceal their identities by using fraudulent names and identification cards. Once identities have been created or stolen from other citizens, drug traffickers use those identifications to falsify records such as Department of Motor Vehicle and phone records for the purpose of theft of services and to evade detection by law enforcement.

m. It is a common practice for drug traffickers to maintain records relating to their drug trafficking activities in their residences, storage lockers, and businesses. Because drug traffickers in many instances will “front” (that is, sell on consignment) controlled substances to their clients, or alternatively, will be "fronted" these items from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. These records include “pay and owe" records to show balances due for drugs sold in the past (pay) and for payments expected (owe) as to the trafficker's suppliers and distributors, telephone and address listings of clients and suppliers, and records of drug proceeds. These records are commonly kept for an extended period of time.

n. Drug traffickers maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other papers relating to the importation, transportation, and distribution of controlled substances. These documents whether in physical or electronic form, are maintained where the traffickers have ready access to them. These documents include travel records, receipts, airline tickets, auto rental agreements, invoices, and other memorandum

disclosing acquisition of assets and personal or business expenses. I also know that one of the most promising places to find such items is within drug traffickers' stash locations, such as storage units.

o. Latent fingerprints and palm prints are frequently found in drug traffickers residences and vehicles, and can be evidence of dominion, control, and possession of stash locations.

38. As described above and in Attachment B, this application seeks permission to search for records that might be found in the **Subject Premises** in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know individuals involved in drug trafficking utilize digital devices, such as cell phones, in furtherance of the Target Offenses. I also know that drug traffickers often store communications, including voice, text, and multi-media messages on their cell phones.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools.

When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, I am aware that digital devices were used to generate communications in furtherance of the Target Offenses. Thus, there is reason to believe that there is a digital device currently located at the **Subject Premises**.

40. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the

purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the **Subject Premises**, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital

device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

41. In most cases, a thorough search of **Subject Premises** for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the **Subject Premises**, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on Premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

42. *Nature of the examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

43. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of

the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

44. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

45. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

46. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

47. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

48. Based on the foregoing, I have probable cause to believe, and I do believe, that HSA and others have committed the Target Offenses, and that contraband, evidence, fruits, and instrumentalities of the offenses, as described above and in Attachment B are presently located at the **Subject Premises**, which is described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the **Subject Premises** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

49. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Peter Sax, who has advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

By phone pursuant to Fed. R. Crim. P. 4.1
Gillian Polinko
Special Agent
Drug Enforcement Administration

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 10:30 a.m./ p.m. on April 28, 2025.

HONORABLE STACIE F. BECKERMAN
United States Magistrate Judge